THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
CHARLESTON DIVISION

INFORMATION ASSOCIATED WITH THE APPLE ID UTILIZING THE NAME RAYNARD SMITH AND EMAIL ADDRESS 1STPLACEMOTORSSC@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC., AN E-MAIL AND CLOUD STORAGE PROVIDER HEADQUARTERED AT 1 INFINITE LOOP M/S 36-SU, CUPERTINO, CA (hereinafter, the "Cloud Storage Provider")	Case No.: 2:22-cr-626

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Hailey Barraco, a Special Agent with Immigration and Customs Enforcement, Homeland Security Investigations ("ICE/HSI"), United States Department of Homeland Security, being first duly sworn, depose and state under oath as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent (SA) with the United States Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) since April of 2019. I am currently assigned to the Assistant Special Agent in Charge (ASAC) Charleston, SC office. I am a graduate of the Federal Law Enforcement Training Center and the HSI Special Agent Training Academy. My responsibilities as a Special Agent include investigating crimes involving the importation and exportation of merchandise contrary to law, controlled substances, and child exploitation. I have also worked, assisted, and observed numerous examples of the sale of counterfeit good and intellectual property rights investigations.

2. Prior to becoming a Special Agent, I was a Financial Crime Investigator (FCI) with the Florida Department of Financial Services (DFS) in Tampa, FL for approximately four years. As an FCI, I worked cases related to welfare fraud and misuse of public benefits. While employed with DFS, I was a member of the United Counsel of Welfare Fraud (UCOWF).

3. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – cloud storage data – which is currently stored at premises controlled by Apple Inc. and described in Attachment B.

4. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of the trafficking of counterfeit goods or services in violation of Title 18, United States Code, Section 2320 are presently located within the cloud storage data.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

IDENTIFICATION OF THE DATA TO BE EXAMINED

6. The property to be searched is an Apple cloud storage account belonging to RAYNARD SMITH utilizing the email address of 1stplacemotorsssc@gmail.com (hereinafter, the SUBJECT STORAGE ACCOUNT).

7. The applied-for warrant would authorize the forensic examination of the data provided by Apple for the purpose of identifying electronically stored data particularly described in Attachment B.

INVESTIGATION OVERVIEW AND STATEMENT OF PROBABLE CAUSE

8. In August 2021, the South Carolina Secretary of State provided information to HSI Charleston regarding a store believed to be selling counterfeit goods such as clothing, shoes, and accessories typically sold in authorized retail stores with trademark brands such as Nike and Jordan. The items were being sold out of a storefront in the Northwoods Mall called GAME OVER SPORTS.

9. An employee with the City of North Charleston verified the business license submitted for the storefront GAME OVER SPORTS was in the name of LANARD SMITH with phone number (843) 532-7178.

10. Records checks of LANARD ISAAC SMITH indicate a prior federal counterfeiting charge and conviction in 2008. Records show that his brother, RAYNARD JACOB SMITH was also involved and convicted of counterfeiting in 2008.

11. A query of the Advanced Targeting System (ATS), which tracks cargo coming in and out of the country shows approximately 48 shipments arriving at GAME OVER SPORTS in the name of RAY SMITH, LARRY SMITH, and GAME OVER SPORTS between April 17, 2021 through November 16, 2021. These shipments are coming from a variety of countries such as

Japan, Malaysia, China, and Hong Kong. The shipments are labeled to contain items such as casual shoes, sports shoes, women's sport suit, men's running shoe, etc.

12. ATS also shows 33 shipments arriving at 600 Westbury Mews Drive, #E, Summerville, SC 29485, in the name of RAYNARD SMITH and ISAAC SMITH between June 2019 and May 2021. These shipments are coming from a variety of countries such as Germany, Japan, Taiwan, China, Hong Kong, Italy, and the United Kingdom. The shipments are labeled to contain items such as men's athletic footwear, men's sport shoes, men's coat, clothes, men's sneakers, cotton mask, etc.

13. Records checks indicate that at least seven of the shippers – for the shipments described in paragraphs 11 and 12 – have been associated with Intellectual Property Violations.

14. On or about September 28, 2021, HSI Charleston utilized a member of the South Carolina Secretary of State to purchase suspected counterfeit apparel from GAME OVER SPORTS. The purchase included a Nike Kobe Bryant Los Angeles Lakers basketball jersey. The Jersey was priced at $150.00. The individual working the store also provided a Lakers facemask for free and failed to charge taxes on the purchase. The total amount paid for the jersey was $150.00. The jersey was reviewed by Investigator Rick Hawks, a representative with Blazer Investigations[1] specializing in Intellectual Property Right matters. Investigator Hawks later notified HSI Charleston the Lakers Jersey purchased from GAME OVER SPORTS was counterfeit.

15. On December 14, 2021, HSI Charleston executed a federal search warrant at GAME OVER SPORTS located at 2150 Northwoods Boulevard, H-600, North Charleston, SC

[1] Blazer Investigations represents a variety of trademark and copyright holders, including, but not limited to, Nike.

29406. Based on confirmation from Blazer Investigations, the merchandise within the store was counterfeit and were seized by HSI Charleston. LANARD SMITH was present at the location and opened the store front at approximately 1030 hours. The retail sales value of the counterfeit merchandise seized from GAME OVER SPORTS has been determined to be $285,815.00.

16. During the December 14, 2021, federal search warrant execution, electronic devices were seized from GAME OVER SPORTS and LANARD SMITH. A subsequent warrant to search the electronic devices was signed by the Honorable Mary Gordon Baker. A review of the electronic devices evidenced conversations between RAYNARD SMITH and LAYNARD SMITH pertaining to the purchase and sale of goods. During their conversations, they sent photographs of sports jerseys and Nike shoes to each other and discussed a warehouse that the shipments from a "jersey connect" can be sent to. LANARD SMITH specifically sent a message to RAYNARD SMITH stating "... I work in that store for you every day for free and lift toys!!! Don't play!!"

17. On February 8, 2022, a federal grand jury returned a three-count indictment against RAYNARD SMITH and LANARD SMITH charging them with Conspiracy to Traffic in Counterfeit Goods pursuant to 18 U.S.C. § 371 and two counts of Trafficking Counterfeit Goods pursuant to 18 U.S.C. § 2320(a)(1).

18. RAYNARD SMITH was interviewed by the United States Probation Office on February 17, 2022, and informed USPO officer Jenniann Benefield that he was self-employed at Game Time, which is located at the subject premises.

19. On February 23, 2022, RAYNARD SMITH appeared for his initial appearance in front of the Honorable Mary Gordon Baker. RAYNARD SMITH was released on bond with

conditions. ECF No. 23. One condition of bond was that the RAYNARD SMITH not violate federal state or local law while on release.

20. On February 28, 2022, HSI Charleston utilized a member of the South Carolina Secretary of State to purchase suspected counterfeit apparel from GAME TIME. A suspected counterfeit Atlanta Falcons facemask was purchased for $11.00. The individual working the store failed to charge taxes on the purchase. The facemask was reviewed by Investigator Rick Hawks, a representative with Blazer Investigations[2] specializing in Intellectual Property Right matters and confirmed to be counterfeit.

21. RAYNARD SMITH was confirmed to be at GAME TIME during the undercover buy on February 28, 2022.

22. On March 1, 2022, the Honorable Molly H. Cherry executed a federal search warrant for GAME TIME.

23. During the execution of the search warrant on March 8, 2022, various devices were recovered and seized from GAME TIME. A subsequent warrant to search the various electronic devices was signed by the Honorable Molly H. Cherry.

24. During review of the subject devices, specifically the Apple iPad (Serial #: DMPDW056LMV9), it was determined that the data on the device had been remotely removed from the device. The Apple ID used on the device was logged out on March 10, 2022, which removed all data from the iPad.

25. Extraction software was able to determine that the Apple ID that removed the data was in the name of RAYNARD SMITH utilizing 1stplacemotorssc@gmail.com. RAYNARD

[2] Blazer Investigations represents a variety of trademark and copyright holders, including, but not limited to, Nike.

SMITH and 1stplacemotorssc@gmail.com are associated with SUBJECT STORAGE ACCOUNT. Based on my training and experience it is believed that the deleted data will be stored in the SUBJECT STORAGE ACCOUNT. In my experience investigating similar crimes, targets often remotely remove data from a device without also deleting the backup on iCloud.

26. Based on my knowledge, training, and experience, individuals who engage in criminal activity which involve the ordering and selling of counterfeit merchandise typically use their cellphones or other forms of electronic devices to access the internet to order the goods. These individuals also keep ledgers or counts as to what was ordered, shipped, and sold on their electronic devices.

27. Also, based on my knowledge, training, and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

28. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

29. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan

to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

BACKGROUND CONCERNING APPLE

30. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

31. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on

multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

e. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

f. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers

running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

32. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

33. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and

utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

34. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

35. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

36. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

CONCLUSION

37. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT STORAGE ACCOUNT, in whatever form they are found.

38. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located in the SUBJECT STORAGE ACCOUNT described in Attachment A. I respectfully request that this Court issue a search warrant for the SUBJECT STORAGE ACCOUNT described in Attachment

A, authorizing the search for evidence more fully described in Attachment B.

39. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

40. Assistant United States Attorney Amy Bower has reviewed this Affidavit.

Respectfully submitted,

Hailey Barraco

Hailey Barraco
Special Agent
Homeland Security Investigations

Sworn to me via telephone or other
Reliable electronic means and signed by me
Pursuant to Fed. R. Crim. P. 4.1 and 4(d) or
41(d)(3), as applicable

May 3, 2022

Molly H. Cherry

The Honorable Molly H. Cherry
United States Magistrate Judge